

security information in order to avoid such accusation and troubles. Such environment impedes improvement of quality of computer program, and is not beneficial for both developers and users.

5 For the developers, on the other hand, it is difficult to collect security information dispersed on the Internet efficiently, and it may take tremendous labor and cost to sort out only useful information from the security information varied very much in quality. It has been attempted to classify
10 the dispersed security information, but successful results are not obtained. At last, the developer are forced to follow the conventional technique of collecting massive amount of security information and sorting out useful information only.

 The invention is devised in the light of such background,
15 and it is hence an object thereof to present a security information mediation apparatus capable of organizing an environment easy for users to present security information, and allowing the developers to collect useful security information at low cost, and its security information
20 mediation method, and a computer-readable recording medium recording a security information mediation program.

SUMMARY OF THE INVENTION

 It is an object of the present invention to provide
25 a method and an apparatus capable of organizing an environment

of the computer program developer), and the usefulness of the security information is judged by the information recipient. Herein, when the security information is judged to be useful, the reply information and payment information
5 are transmitted from the information recipient's terminal.

Consequently, when the reply information and payment information are received by the receiving unit, the second transfer unit transfers the reply information and payment information to the information contributor's terminal. As
10 a result, the information contributor understands that the presented security information was useful, and recognizes payment for presentation of security information.

Thus, the security information from the information contributor is directly presented to the information
15 recipient side, and reward is paid to the user presenting useful security information, and therefore it is easier for the information contributor (user) to present security information, while the information recipient (for example, developer) can collect useful security information at low
20 cost.

The security information mediation method according to another aspect of the present invention comprises a registering step of registering security information presented from the information contributor's terminal, a
25 first transfer step of transferring the security information

registered at the registering step to the information recipient's terminal for judging the usefulness of the security information, a receiving step of receiving the reply information showing the usefulness of the security information and the payment information about payment of the information presentation fee of the corresponding security information from the information recipient's terminal, and a second transfer step of transferring the reply information and payment information to the information contributor's terminal.

When the security information is presented from the information contributor (user), the security information is registered at the registering step. As a result, the first transfer step transfers the security information to the information recipient's terminal (for example, the terminal of the computer program developer), and the usefulness of the security information is judged by the information recipient. Herein, when the security information is judged to be useful, the reply information and payment information are transmitted from the information recipient's terminal.

Consequently, when the reply information and payment information are received at the receiving step, the second transfer step transfers the reply information and payment information to the information contributor's terminal. As
25 a result, the information contributor understands that the

presented security information was useful, and recognizes payment for presentation of security information.

Thus, the security information from the information contributor is directly presented to the information recipient side, and reward is paid to the user presenting useful security information, and therefore it is easier for the information contributor (user) to present security information, while the information recipient (for example, developer) can collect useful security information at low cost.

Other objects and features of this invention will become apparent from the following description with reference to the accompanying drawings.

15 BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram showing a configuration of a first embodiment of the invention.

Fig. 2A shows the security information 40, Fig. 2B shows the reply information 41A, Fig. 2C shows the reply information 41B, and Fig. 2D shows the payment information 42 shown in Fig. 1.

Fig. 3 is a flowchart for explaining the operation in the first embodiment.

Fig. 4 is a block diagram showing a configuration of a second embodiment of the invention.

a fourth embodiment of the invention.

Fig. 13A shows a data structure of the reply information database 1002, Fig. 13B shows a data structure of the disclosed information database 1004, and Fig. 13B shows the patch information 1100 shown in Fig. 12.

Fig. 14 is a diagram showing an example of information disclosure screen 1200 in the fourth embodiment.

Fig. 15 is a flowchart for explaining the operation in the fourth embodiment.

Fig. 16 is a flowchart for explaining the operation of information disclosure unit 1003 shown in Fig. 12.

Fig. 17 is a block diagram showing a modified example of the first to fourth embodiments of the invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Four preferred embodiments of the security information mediation apparatus, security information mediation method, and computer-readable recording medium recording a security information mediation program of the invention are explained in detail below with reference to the attached drawings.

Fig. 1 is a block diagram showing a configuration of a first embodiment of the invention. As shown in this figure, a user client 11 is a computer terminal operated by a user 10, and is accessible to a security information mediation apparatus 20 through a network 12. The user 10 is a person

using various computer programs developed by developer 31A and developer 31B mentioned below, and other developers. The user 10 is also a learned person having enough knowledge for discovering bugs and security holes of computer programs, and presenting them as security information.

The user client 11 has a function of registering security information 40 in the security information mediation apparatus 20 through the network 12, and a function of receiving reply information 41A and payment information 42 from the security information mediation apparatus 20 when the security information 40 is useful. This security information 40 is the information presented to the developer of the computer program if the user 10 discovers a security hole in the computer program.

Specifically, the security information 40 shown in Fig. 2A is composed of "registering person" (user 10) and "content of security information" (bug problem of software X). The "registering person" is the information showing the person who has registered the security information, and the "content of security information" is the information showing the specific content of the security information.

The reply information 41A is the information replied from the developer to the user 10 in the case the security information 40 is judged to be valid by the developer. Specifically, the reply information 41A shown in Fig. 2B is

composed of "replying person" (developer 31A), "judging result" (valid), "registering person" (user10), and "content of security information" (bug problem of software X).

The "replying person" is the information showing the
5 developer replying to the security information registered
in the security information mediation apparatus 20, and the
"judging result" is the information showing whether the
security information is valid or not. The "registering
person" is the information showing the person who has
10 registered the security information, and the "content of
security information" is the information showing the specific
content of the security information.

The payment information 42 is the information about the amount of money to be paid from the developer 31A to the user 10 as the reward for presenting the security information 40 when the security information 40 is judged to be valid at the developer 31A side, and the method of payment. Specifically, the payment information 42 shown in Fig. 2D is composed of "amount paid" (10000 yen), "paid to" (user 10), "paid by" (developer 31A), and "paying method" (electronic settlement).

The "amount paid" is the information about the amount to be paid from the developer 31A to the user 10 as the reward for presentation of the security information 40. The "paid to" is the information showing to whom the amount is paid.

000221"5496E/60

The "paid by" is the information showing who is to pay the amount. The "paying method" is the information showing the method of payment of the amount to the user. In the first embodiment, the "paying method" is electronic settlement, 5 but other method of payment is also possible such as transfer to bank account.

The security information mediation apparatus 20 is a server mediating security information between the user 10 and developers 31A and 31B, and is interposed between the network 12 and network 32. The security information mediation apparatus 20 is accessed by the user client 11 and developer clients 30A and 30B.

In the security information mediation apparatus 20, a security information registering unit 21 has a function of registering the security information 40 from the user client 11 into a security information database 22. Actually, 15 aside from the user client 11, multiple user clients are connected to the network 12. Therefore, the security information registering unit 21 also has a function of registering the security information from other user clients 20 into the security information database 22.

A transfer unit 23 has a function of transferring the security information registered by the security information registering unit 21 to the developer clients 30A and 30B 25 through the network 32. The network 32 is for connecting

the security information mediation apparatus 20 and the developer clients 30A and 30B. The developer client 30A is a computer terminal installed at the side of the developer 31A, that is, the vendor of the computer program. The
5 developer client 30B is a computer terminal installed at the side of the developer 31B, that is, the vendor of the computer program.

The developer client 30A receives the security information 40 from the transfer unit 32, and transmits the
10 reply information 41A (see Fig. 2B) and payment information 42 (see Fig. 2D) to the security information mediation apparatus 20. Similarly, the developer client 30B receives the security information 40 from the transfer unit 23, and transmits the reply information 41B to the security
15 information mediation apparatus 20.

In the shown example, payment information is not transmitted from the developer client 30B. This is because the security information 40 is invalid for the developer 31B, and payment as reward does not arise. That is, the "judging
20 result" of reply information 41A (see Fig. 2B) is valid, while the "judging result" of the reply information 41B (see Fig. 2C) is invalid. In this case, the "replying person" of reply information 41B is the developer 31B.

In the security information mediation apparatus 20,
25 a reply information registering unit 24 has a function of

000221" 5496E/50

registering reply information 41A, payment information 42,
and reply information 41B sent from the developer client 30A
and developer client 30B through the network 32 into the reply
information database 25. A transfer unit 26 has a function
5 of transferring the reply information judged to be valid of
the reply information registered in the reply information
registering unit 24 (reply information 41A in the shown
example), and payment information about the reply information
(payment information 42 in this example) to the corresponding
10 user client (user client 11 in the example) through the network
12.

The operation of the first embodiment is explained below
by referring to the flowchart in Fig. 3. At step SA1 in the
diagram, the security information registering unit 21 judges
15 if the security information is received from the user client
11 or not, and in this case it is judged No. Herein, the
user 10 discovering a bug (security hole) in software X creates
security information 40 shown in Fig. 2A with the aid of the
user client 11. By the operation by the user 10, the security
20 information 40 is transmitted from the user client 11 to the
security information mediation apparatus 20.

Receiving this security information 40, the security
information registering unit 21 judges Yes at step SA1. At
step SA2, the security information registering unit 21
25 registers the security information 40 in the security

information database 22. At step SA3, the security information registering unit 21 transfers the security information 40 to the transfer unit 23. As a result, the transfer unit 23 transfers the security information 40 parallel to the developer clients 30A and 30B. At step SA4, the reply information registering unit 24 judges if the reply information is received or not, and in this case it is judged No.

When the security information 40 is received by the developer clients 30A and 30B, the developers 31A and 31B individually judge if the security information 40 is valid information or not. Herein, the security information 40 is "valid" when it is judged to contribute to upgrading of the software X and be worth paying due amount to the user 10 as the reward for presentation.

In this case, suppose the developer 31A judges the security information 40 to be valid. At the developer 31A, using the developer client 30A, the reply information 41A (see Fig. 2B) and payment information 42 (see Fig. 2D) are created, and they are sent to the security information mediation apparatus 20. The reply information 41A and payment information 42 are received in the reply information registering unit 24 of the security information mediation apparatus 20 through the network 32.

As a result, the reply information registering unit

24 judges Yes at step SA4. At step SA5, the reply information registering unit 24 judges if the result of judgment of the reply information 41A shown in Fig. 2B is valid or not, and it is judged Yes herein. At step SA6, the reply information registering unit 24 judges if the payment information corresponding to the received reply information 41A is received or not, and it is judged Yes in this case. If judged No at step SA6, the reply information registering unit 24 repeats the same judgment.

At step SA7, the reply information registering unit 24 registers the reply information 41A and payment information 42 in the replay information database 25. At step SA8, the reply information registering unit 24 transfers the reply information 41A and payment information 42 to the transfer unit 26. As a result, the transfer unit 26 transfers the reply information 41A and payment information 42 to the user client 11 through the network 12.

When the reply information 41A and payment information 42 are received in the user client 11, the user client 11 informs the user 10 of the reply information 41A and payment information 42. As a result, the user 10 understands that the security information 40 the user has presented was useful, and recognizes that 10000 yen is paid from the developer 31A by electronic settlement.

On the other hand, suppose the developer 31B had judged

the security information 40 invalid. Being "invalid" means that the software X in question is indifferent to the developer 31B, and it is not worth paying due amount to the user as reward for presentation. In this case, at the developer 31B, using the developer client 30B, invalidity reply information 41B (see Fig. 2C) is created, and transmitted to the security information mediation apparatus 20. This reply information 41B is received in the reply information registering unit 24 of the security information mediation apparatus 20 through the network 32.

As a result, the reply information registering unit 24 judges Yes at step SA4. At step SA5, the reply information registering unit 24 judges if the result of judgment of the reply information 41B shown in Fig. 2C is valid or not, and it is judged No in this case. At step SA9, the reply information 41B is registered in the reply information database 25.

As explained herein, according to the first embodiment, the security information 40 from the user 10 is directly presented to the developer 31A and developer 31B, and reward is paid to the user presenting useful security information, and therefore the environment is easy for the user 10 to present security information, while the developer 31A and developer 31B can collect useful security information at low cost.

Fig. 4 is a block diagram showing a configuration of

a second embodiment of the invention. As shown in this figure, a user client 101A is a computer terminal operated by a user 100A, and is accessible to a security information mediation apparatus 200 through a network 102. The user 100A is a person using various computer programs developed by developer 301 mentioned below, and other developers. The user 100A is also a learned person having enough knowledge for discovering bugs and security holes of computer programs, and presenting them as security information.

The user client 101A, same as the user client 11 (see Fig. 1), has a function of registering security information 400A in the security information mediation apparatus 200 through the network 102, and a function of receiving (in the diagram, reply information 401A and payment information 402) from the security information mediation apparatus 200.

This security information 400A is the information presented to the developer of the computer program if the user 100A discovers a security hole in the computer program, and it is composed same as the security information 40 (see Fig. 2A). Specifically, the security information 400A shown in Fig. 5A is composed of "registering person" (user 100A) and "content of security information" (bug problem QA of software X).

The reply information 401A, same as the reply information 41A (see Fig. 2B), is the information replied

from the developer to the user 100A in the case the security information 400A is judged to be valid by the developer. Specifically, the reply information 401A shown in Fig. 5C is composed of "replying person" (developer 301), "judging result" (valid), "registering person" (user 100A), and "content of security information" (bug problem QA of software X).

The payment information 402, same as the payment information 42 (see Fig. 2D), is the information about the amount of money to be paid from the developer 301 to the user 100A as the reward for presenting the security information 400A when the security information 400A is judged to be valid at the developer 301 side, and the method of payment. Specifically, the payment information 402 shown in Fig. 5E is composed of "amount paid" (10000 yen), "paid to" (user 100A), "paid by" (developer 301), and "paying method" (electronic settlement).

On the other hand, a user client 101B is a computer terminal operated by a user 100B, and is accessible to the security information mediation apparatus 200 through the network 102. The user 100B, same as the user 100A, is a person using various computer programs developed by developer 301 mentioned below, and other developers. The user 100B is also a learned person having enough knowledge for discovering bugs and security holes of computer programs, and presenting them

as security information.

The user client 101B, same as the user client 101A, has a function of registering security information 400B in the security information mediation apparatus 200 through the network 102, and a function of receiving (in the diagram, reply information 401B) from the security information mediation apparatus 200.

This security information 400B is the information presented to the developer of the computer program if the user 100B discovers a security hole in the computer program, and it is composed same as the security information 40 (see Fig. 2A). Specifically, the security information 400B shown in Fig. 5B is composed of "registering person" (user 100B) and "content of security information" (bug problem QB of software X).

The reply information 401B is the information replied from the developer to the user 100B in the case the security information 400B is judged to be invalid by the developer. Specifically, the reply information 401B shown in Fig. 5D is composed of "replying person" (developer 301), "judging result" (invalid), "registering person" (user 100B), and "content of security information" (bug problem QB of software X).

The security information mediation apparatus 200 is a server mediating security information between the users

100A and 100B and the developer 301, and is interposed between the network 102 and network 302. The security information mediation apparatus 200 is accessed by the user clients 101A and 101B and the developer client 300.

5 In the security information mediation apparatus 200, a receiving unit 201 has a function of receiving the security information 400A and 400B from the user clients 101A and 101B. An information management unit 202 has a function of managing the security information 400A and 400B received in the
10 receiving unit 201, reply information 401A, 401B and payment information 402 received in a receiving unit 206 described below. The function of the information management unit 202 is explained later.

A transfer unit 205 has a function of transferring the
15 security information registered by the information management unit 202 to the developer client 300 through the network 302. The network 302 is for connecting the security information mediation apparatus 200 and the developer client 300. The developer client 300 is a computer terminal
20 installed at the side of the developer 301, that is, the vendor of the computer program.

The developer client 300 receives the security information 400A and 400B from the transfer unit 205, and transmits the reply information 401A (see Fig. 5C), reply
25 information 401B (see Fig. 5D), and payment information 402

(see Fig. 5E) to the security information mediation apparatus 200.

In the shown example, payment information corresponding to the security information 400B is not transmitted from the developer client 300. This is because the security information 400B is invalid for the developer 301, and payment as reward does not arise. That is, the "judging result" of reply information 401A (see Fig. 5C) is valid, while the "judging result" of the reply information 401B (see Fig. 5D) is invalid. In this case, the "replying person" of both reply information 401A and 401B is the developer 301.

In the security information mediation apparatus 200, a receiving unit 206 has a function of receiving the reply information and payment information (in the diagram, reply information 401A, 401B, and payment information 402) transmitted from the developer client 300 through the network 302. The information management unit 202 has a function of registering the security information (in the diagram, security information 400A and 400B) received in the receiving unit 201 in the security information database 203 shown in Fig. 6A.

The security information database 203 is composed of "registration No." given in the order of registration of security information, "date of registration", "registering

person", and "content of security information". In the diagram, a record of "registration No." = 3 corresponds to the security information 400A (see Fig. 5A), and a record of "registration No." = 4 corresponds to the security information 400B (see Fig. 5B).

The information management unit 202 also has a function of registering the reply information received in the receiving unit 206 (in the diagram, reply information 401A and 401B) in a reply information database 204 shown in Fig. 6B. This reply information database 204 is composed of "reply No." given in the order of registration of reply information, "date of reply", "registration No." (see Fig. 6A), "replying person", and "judging result". In the diagram, a record of "reply No." = 3 corresponds to the reply information 401A (see Fig. 5C), and a record of "reply No." = 4 corresponds to the reply information 401B (see Fig. 5D).

The information management unit 202 further transfers the reply information of which result of judgment is valid or invalid (in the diagram, reply information 401A and reply information 401B), and payment information (in the diagram, payment information 402) to a transfer unit 207. The transfer unit 207 has a function of transferring the reply information and payment information from the information management unit 202 to the corresponding user client through the network 102.

The operation of the second embodiment is explained

below by referring to the flowchart in Fig. 7. At step SB1 in the diagram, the information management unit 202 judges if the security information is received in the receiving unit 201 or not, and in this case it is judged No.

5 Herein, the user 100A discovering a bug (security hole) in software X creates security information 400A shown in Fig. 5A with the aid of the user client 101A. By the operation by the user 100A, the security information 400A is transmitted from the user client 101A to the security information
10 mediation apparatus 200.

 Receiving this security information 400A in the receiving unit 201, the information management unit 202 judges Yes at step SB1. At step SB2, the information management unit 202 retrieves the security information database 203 shown
15 in Fig. 6A, using the "registering person" and "content of security information" of the security information 400A as the key. In this case, suppose only records of "registration No." = 1 and 2 are present in the security information database 203.

20 At step SB3, the information management unit 202 judges if the retrieval is successful or not, that is, whether the same content as the security information 400A is registered in the security information database 203 or not, and if judged Yes, at step SB11, the information management unit 202 rejects
25 registration. In this case, the information management unit

202 judges No at step SB3.

At step SB4, the information management unit 202 registers the security information 400A in the security information database 203 (see Fig. 6A). As a result, in the security information database 203, a record of "registration No." = 3 (corresponding to security information 400A) is added.

At step SB5, the information management unit 202 transfers the security information 400A to the transfer unit 205. The transfer unit 205 transfers the security information 400A to the developer client 300 through the network 302. At step SB6, the information management unit 202 judges if the reply information is received in the receiving unit 206 or not, and it is judged No in this case.

When the security information 400A is received by the developer client 300, the developers 301 judges if the security information 400A is valid information or not. In this case, suppose the developer 301 judges the security information 400A to be valid. At the developer 301, using the developer client 300, the reply information 401A (see Fig. 5C) and payment information 402 (see Fig. 5E) are created, and they are sent to the security information mediation apparatus 200. The reply information 401A and payment information 402 are received in the receiving unit 206 of the security information mediation apparatus 200 through the

network 302.

As a result, the information management unit 202 judges Yes at step SB6. At step SB7, the information management unit 202 registers the reply information 401A in the reply information database 204 (see Fig. 6B). Consequently, a record of "reply No." = 3 (corresponding to the reply information 401A) is added to the reply information database 204.

At step SB8, the information management unit 202 judges if the result of judgment of the reply information 401A shown in Fig. 5C is valid or not, and it is judged Yes herein. At step SB9, the information management unit 202 judges if the payment information 402 corresponding to the reply information 401A is received in the receiving unit 206 or not, and it is judged Yes in this case. If judged No at step SB9, the information management unit 202 repeats the same judgment.

At step SB10, the information management unit 202 transfers the reply information 401A and payment information 402 to the transfer unit 207. As a result, the transfer unit 207 transfers the reply information 401A and payment information 402 to the user client 101A through the network 102.

When the reply information 401A and payment information 402 are received in the user client 101A, the user client

101A informs the user 100A of the reply information 401A and payment information 402. As a result, the user 100A understands that the security information 400A the user has presented was useful, and recognizes that 10000 yen is paid
5 from the developer 301 by electronic settlement.

On the other hand, the user 100B discovering a bug (security hole) in software X creates security information 400B shown in Fig. 5B with the aid of the user client 101B. By the operation by the user 100B, the security information
10 400B is transmitted from the user client 101B to the security information mediation apparatus 200.

Receiving this security information 400B in the receiving unit 201, the information management unit 202 judges Yes at step SB1. At step SB2, the information management
15 unit 202 retrieves the security information database 203, using the "registering person" and "content of security information" of the security information 400B as the key. In this case, suppose only records of "registration No." = 1 to 3 are present in the security information database 203.

20 At step SB3, the information management unit 202 judges if the retrieval is successful or not, and it is judged No. At step SB4, the information management unit 202 registers the security information 400B in the security information database 203 (see Fig. 6A). As a result, in the security
25 information database 203, a record of "registration No." =

4 (corresponding to security information 400B) is added.

At step SB5, the information management unit 202 transfers the security information 400B to the transfer unit 205. The transfer unit 205 transfers the security information 400B to the developer client 300 through the network 302. At step SB6, the information management unit 202 judges if the reply information is received in the receiving unit 206 or not, and it is judged No in this case.

When the security information 400B is received by the developer client 300, the developers 301 judges if the security information 400B is valid information or not. In this case, suppose the developer 301 judges the security information 400B to be invalid. At the developer 301, using the developer client 300, the reply information 401B as the reject message (see Fig. 5D) is created, and sent to the security information mediation apparatus 200.

The reply information 401B is received in the receiving unit 206 of the security information mediation apparatus 200 through the network 302. As a result, the information management unit 202 judges Yes at step SB6. At step SB7, the information management unit 202 registers the reply information 401B in the reply information database 204 (see Fig. 6B). Consequently, a record of "reply No." = 4 (corresponding to the reply information 401B) is added to the reply information database 204.

At step SB8, the information management unit 202 judges if the result of judgment of the reply information 401B shown in Fig. 5D is valid or not, and it is judged No herein. At step SB12, the information management unit 202 transfers the
5 reply information 401B as reject message to the transfer unit 207. As a result, the transfer unit 207 transfers the reply information 401B to the user client 101B through the network 102. When the reply information 401B is received in the user client 101B, the user client 101B informs the user 100B of
10 the reply information 401B. As a result, the user 100B understands that the security information 400B the user has presented was invalid.

As explained herein, according to the second embodiment, since the reply information 401B showing invalidity of the
15 security information 400B presented from the user 100B is transferred to the user client 101B, it is effective to improve the service for the user interested in the manner of use (valid or invalid) of the presented security information.

Further, only when the security information (security
20 information 400A, 400B) presented from the users (user 100A, user 100B) is new, such security information is transferred to the developer client 300, and hence it saves the wasteful time of transferring unnecessary security information to the developer client 300, so that the security information may
25 be collected efficiently.

Fig. 8 is a block diagram showing a configuration of a third embodiment of the invention. As shown in this figure, a user client 501 is a computer terminal operated by a user 500, and is accessible to a security information mediation apparatus 600 through a network 502.

The user 500 is a person using various computer programs developed by developers 7011A and 701B mentioned below, and other developers. The user 500 is also a learned person having enough knowledge for discovering bugs and security holes of computer programs, and presenting them as security information.

The user client 501, same as the user client 11 (see Fig. 1), has a function of registering security information 800 in the security information mediation apparatus 600 through the network 502, and a function of receiving information (in the diagram, reply information 801 and payment information 802) from the security information mediation apparatus 600.

The security information 800 is the information to be presented to the developer of the computer program if the user 500 discovers a security hole in the computer program, and it is composed same as the security information 40 (see Fig. 2A). Specifically, the security information 800 shown in Fig. 9A is composed of "registering person" (user 500) and "content of security information" (bug problem of software

X) .

000221"54956260

The reply information 801, same as the reply information 41A (see Fig. 2B), is the information replied from the developer to the user 500 in the case the security information 800 is judged to be valid by the developer. Specifically, the reply information 801 shown in Fig. 9B is composed of "replying person" (developer 701A), "judging result" (valid), "registering person" (user 500), "classification" (A) and "content of security information" (bug problem of software X). Herein, "classification" is the information showing the corresponding classification item of the content of the security information.

The payment information 802, same as the payment information 42 (see Fig. 2D), is the information about the amount of money to be paid from the developer 701A to the user 500 as the reward for presenting the security information 800 when the security information 800 is judged to be valid at the developer 701A side, and the method of payment. Specifically, the payment information 802 shown in Fig. 9C is composed of "amount paid" (10000 yen), "paid to" (user 500), "paid by" (developer 701A), and "paying method" (electronic settlement).

The security information mediation apparatus 600 is a server mediating security information between the user 500 and developers 701A and 701B, and is interposed between the

network 502 and network 702. The security information mediation apparatus 600 is accessed by the user client 501 and developer clients 700A and 700B.

In the security information mediation apparatus 600,
5 a receiving unit 601 has a function of receiving the security information 800 from the user client 501. An information management unit 602 has a function of managing the security information 800 received in the receiving unit 601, reply
10 receiving unit 607 described below. The function of the information management unit 602 is explained later.

A transfer unit 605 has a function of transferring the security information registered by the information management unit 602 to the developer clients 700A and 700B
15 through the network 702. The transfer unit 605 also has a function of receiving the classification information 803A and 803B from the developer clients 700A and 700B, and registering them in the classification information database 606.

20 The classification information 803A is the information showing the classification of security information required at the developer 701A. Specifically, the classification information 803A shown in Fig. 9D is composed of "developer" (developer 701A) and "classification" (A). Therefore, the
25 developer 701A requires only the security information

000221 5495E/60
belonging to classification A, and does not require security
information belonging to other classification. In other
words, the classification information 803A is filtering
information for extracting security information required at
5 the developer 701A, out of a multiplicity of security
information registered in the security information mediation
apparatus 600.

On the other hand, the classification information 803B,
like the classification information 803A, is the information
10 showing the classification of security information required
at the developer 701B. Specifically, the classification
information 803B shown in Fig. 9E is composed of "developer"
(developer 701B) and "classification" (B).

Therefore, the developer 701B requires only the
15 security information belonging to classification B, and does
not require security information belonging to other
classification. Thus, same as the classification
information 803A, the classification information 803B is also
filtering information for extracting security information
20 required at the developer 701B, out of a multiplicity of
security information registered in the security information
mediation apparatus 600.

The classification information database 606 is, as
shown in Fig. 10C, composed of "developer" and
25 "classification". In this classification information

database 606, the record of "developer" (= developer 701A) corresponds to the classification information 803A (see Fig. 9D), and the record of "developer" (= developer 701B) corresponds to the classification information 803B (see Fig. 9E).

The network 702 is for connecting the security information mediation apparatus 600 and the developer clients 700A and 700B. The developer client 700A is a computer terminal installed at the side of the developer 701A, that is, the vendor of the computer program. The developer client 700B is a computer terminal installed at the side of the developer 701B, that is, the vendor of the computer program.

The developer client 700A transmits the classification information 803A (see Fig. 9D) to the transfer unit 605, and receives the security information (in the diagram, security information 800) corresponding to the classification information 803A. Also, when the security information is valid, the developer client 700A transmits the reply information 801 (see Fig. 9B) and payment information 802 (see Fig. 9C) to the security information mediation apparatus 600.

On the other hand, the developer client 700B transmits the classification information 803B (see Fig. 9E) to the transfer unit 605, and receives the security information corresponding to the classification information 803B. Also,

when the security information is valid, same as the developer client 700A, the developer client 700B transmits the reply information and payment information to the security information mediation apparatus 600.

5 In the security information mediation apparatus 600, the receiving unit 607 has a function of receiving the reply information and payment information (in the diagram, reply information 801 and payment information 802) transmitted from the developer clients 700A, 700B through the network 702.

10 The information management unit 602 has a function of registering the security information (in the diagram, security information 800) received in the receiving unit 601 in the security information database 603 shown in Fig. 10A.

 The security information database 603 is composed of

15 "registration No." given in the order of registration of security information, "date of registration", "registering person", "classification" showing the classification of security information, and "content of security information". In the diagram, a record of "registration No." = 3 corresponds

20 to the security information 800 (see Fig. 9A).

 The information management unit 602 also has a function of registering the reply information (in the diagram, reply information 801) received in the receiving unit 607 in a reply information database 604 shown in Fig. 10B. This reply

25 information database 604 is composed of "reply No." given

in the order of registration of reply information, "date of
reply", "registrationNo." (see Fig. 10A), "replyingperson",
"classification" (see Fig. 10A), and "judging result". In
the diagram, a record of "reply No." = 3 corresponds to the
5 reply information 801 (see Fig. 9B).

The information management unit 602 further transfers
the reply information of which result of judgment is valid
or invalid (in the diagram, reply information 801), and
payment information (in the diagram, payment information 802)
10 to a transfer unit 608. The transfer unit 608 has a function
of transferring the reply information and payment information
from the information management unit 602 to the corresponding
user client through the network 502.

The operation of the third embodiment is explained below
15 by referring to the flowchart in Fig. 11. At step SC1 in
the diagram, the transfer unit 605 executes classification
registration process. Specifically, the transfer unit 605
receives the classification information 803A (see Fig. 9D)
and classification information 803B (see Fig. 9E) from the
20 developer clients 700A and 700B through the network 702, and
registers them in the classification information database
606 (see Fig. 10C).

After the classification information registration
process, at step SC2, the information management unit 602
25 judges if the security information is received in the

800, executes the classification process by judging the classification of the security information 800 in the preset classes (for example, A to Z).

In this case, suppose the information management unit
5 602 has judged the security information 800 to be
classification A. At step SC6, the information management
unit 602 registers the security information 800 in the
security information database 603 (see Fig. 10A)
corresponding to classification A. As a result, in the
10 security information database 603, a record of "registration
No." = 3 (corresponding to security information 800) is added.

At step SC7, the information management unit 602
accesses the classification information database 606 by way
of the transfer unit 605, and retrieves the classification
15 information database 606 shown in Fig. 10C, using
classification A of the security information 800 as the key.
At step SC8, the information management unit 602 judges
whether same classification as classification A of the
security information 800 is present or not in the
20 classification information database 606.

In this case, since the classification (A) of "the
developer" (developer 701A) in the classification
information database 606 coincides with the classification
A of the security information 800, the information management
25 unit 602 judges Yes at step SC8. If judged No at step SC8,

the information management unit 602 repeats the process after step SC2.

At step SC9, the information management unit 602 transfers the security information 800 addressed to the developer client 700A to the transfer unit 605. As a result, the transfer unit 605 transfers the security information 800 to the developer client 700A. In this case, the security information 800 is not transferred to the developer client 700B. At step SC10, the information management unit 602 judges if the reply information is received in the receiving unit 607, and it is judged No in this case.

When the security information 800 is received by the developer client 700A, the developers 701A judges if the security information 800 is valid information or not. In this case, suppose the developer 701A judges the security information 800 to be valid. At the developer 701A, using the developer client 700A, the reply information 801 (see Fig. 9B) and payment information 802 (see Fig. 9C) are created, and they are sent to the security information mediation apparatus 600. The reply information 801 and payment information 802 are received in the receiving unit 607 of the security information mediation apparatus 600 through the network 702.

As a result, the information management unit 602 judges Yes at step SC10. At step SC11, the information management

unit 602 registers the reply information 801 in the reply
information database 604 (see Fig. 10B). Consequently, a
record of "reply No." = 3 (corresponding to the reply
information 801) is added to the reply information database
5 604.

At step SC12, the information management unit 602 judges
if the result of judgment of the reply information 801 shown
in Fig. 9B is valid or not, and it is judged Yes herein. At
step SC13, the information management unit 602 judges if the
10 payment information 802 corresponding to the reply
information 801 is received in the receiving unit 607 or not,
and it is judged Yes in this case. If judged No at step SC13,
the information management unit 602 repeats the same judgment.

At step SC14, the information management unit 602
15 transfers the reply information 801 and payment information
802 to the transfer unit 608. As a result, the transfer unit
608 transfers the reply information 801 and payment
information 802 to the user client 501 through the network
502.

20 When the reply information 801 and payment information
802 are received in the user client 501, the user client 501
informs the user 500 of the reply information 801 and payment
information 802. As a result, the user 500 understands that
the security information 800 the user has presented was useful,
25 and recognizes that 10000 yen is paid from the developer 701A

by electronic settlement.

On the other hand, if judged No at step SC12, that is, when the reply information of "judging result" = "invalid" is received in the receiving unit 607, at step SC16, the information management unit 602 transfers the reply
5 information as reject message to a transfer unit 608. As a result, the transfer unit 608 transfers the reply information (reject message) to the user client 501 through the network 502. When this reply information (reject
10 message) is received in the user client 501, the user client 501 informs the user 500 of the reply information. As a result, the user 500 understands that the presented security information was invalid.

As explained herein, according to the third embodiment,
15 by registering the classification information of the security information desired by the developer 701A and developer 701B in the classification information database 606, and transferring the security information 800, for example, to the developer client 700A only when the classification
20 information coincides with the classification result of the security information 800 presented from the user 500, it saves the wasteful time of transferring unnecessary security information, so that the security information may be collected more efficiently.

25 In the third embodiment, the security information is

shared between the concerned parties (user and developer),
but the security information or patch information for
correcting the computer program may be disclosed to a third
party or general users. This case is explained as a fourth
5 embodiment.

Fig. 12 is a block diagram showing a configuration of
the fourth embodiment of the invention. In this figure, the
same parts corresponding to the components in Fig. 8 are
identified with same legends. As shown in this figure, a
10 security information mediation apparatus 1000 is provided
instead of the security information mediation apparatus 600
shown in Fig. 8.

In this security information mediation apparatus 1000,
an information management unit 1001 and a reply information
15 database 1002 are provided instead of the information
management unit 602 and reply information database 604 shown
in Fig. 8. Further, in the security information mediation
apparatus 1000, an information disclosing unit 1003 and a
disclosed information database 1004 are newly provided. In
20 Fig. 12, moreover, a user client 901 to be operated by a user
900 is provided.

The security information mediation apparatus 1000 is
a server mediating security information or patch information
between the users 500 and 900 and developers 701A and 701B,
25 and is interposed between the network 502 and network 702.

The security information mediation apparatus 1000 is accessed by the user client 501, user client 901, and developer clients 700A and 700B.

In the security information mediation apparatus 1000,
5 a receiving unit 607 receives patch information 1100 from the developer client 700A, in addition to the reply information 801 and payment information 802 mentioned above. This patch information 1100 is, as shown in Fig. 13C, composed of "reply No." (3) Corresponding to the reply information
10 801, "replying person" (developer 701A), and patch program, and this is the information for correcting the computer program having a security hole.

The information management unit 1001 has a function of registering the security information (in the diagram, security information 800) received in the receiving unit 601
15 in the security information database 603. The information management unit 1001 also has a function of registering the reply information (in the diagram, reply information 801) received in the receiving unit 607 in the reply information
20 database 1002 shown in Fig. 13A.

This reply information database 1002, like the reply information database 604 (see Fig. 10B), is divided into the columns of "reply No." given in the order of registration of reply information, "date of reply", "registration No.",
25 "replying person", "classification", and "judging result".

The reply information database 1002 also has a column for "correcting method". This "correcting method" is the information showing the method of correction (for example, patch) of computer program having a security hole. In the
5 diagram, a record of "reply No." = 3 corresponds to the reply information 801 (see Fig. 9B).

The information management unit 1001, like the information management unit 602, transfers the reply information (in the diagram, reply information 801) of which
10 result of judgment is valid or invalid, and the payment information (in the diagram, payment information 802) to the transfer unit 608. Also, the information management unit 1001 transfers the security information, reply information and patch information to the information disclosing unit 1003.

15 The information disclosing unit 1003 has a function of disclosing security information, reply information, and patch information to the user client 901 of the user 900 or a third party through an information disclosing screen 1200 (see Fig. 14) on the web site. The information disclosing
20 unit 1003 registers the security information, reply information and patch information from the information management unit 1001 in the disclosed information database 1004 shown in Fig. 13B.

This disclosed information database 1004 is, same as
25 the reply information database 1002 (see Fig. 13A), composed

of "reply No.", "classification", "content of security information", "replying person", "correcting method", "security information pointer", and "patch information pointer". The "security information pointer" is a pointer
5 indicating a region in which the security information is actually stored, and the "patch information pointer" is a pointer indicating a region in which the patch information is actually stored.

The operation of the fourth embodiment is explained
10 below by referring to the flowchart in Fig. 15. At step SD1 in the diagram, the transfer unit 605, same as at step SD1 (see Fig. 11), registers the classification information 803A (see Fig. 9D) and classification information 803B (see Fig. 9E) in the classification information database 606 (see Fig. 10C).

15 At step SD2, the information management unit 1001 judges if the security information is received in the receiving unit 601 or not, and in this case it is judged No. Herein, the user 500 discovering a bug (security hole) in software X creates security information 800 shown in Fig. 9A with the
20 aid of the user client 501. By the operation by the user 500, the security information 800 is transmitted from the user client 501 to the security information mediation apparatus 1000.

Receiving this security information 800 in the
25 receiving unit 601, the information management unit 1001

judges Yes at step SD2. At step SD3, the information management unit 1001 retrieves the security information database 603 shown in Fig. 10A, using the "registering person" and "content of security information" of the security information 800 as the key. In this case, suppose only records of "registration No." = 1 and 2 are present in the security information database 603.

At step SD4, the information management unit 1001 judges if the retrieval is successful or not, that is, whether the same content as the security information 800 is registered in the security information database 603 or not, and if judged Yes, at step SD19, the information management unit 1001 rejects registration. In this case, the information management unit 1001 judges No at step SD4.

At step SD5, the information management unit 1001, on the basis of the content of the received security information 800, executes the classification process by judging the classification of the security information 800 in the preset classes (for example, A to Z).

In this case, suppose the information management unit 1001 has judged the security information 800 to be classification A. At step SD6, the information management unit 1001 registers the security information 800 in the security information database 603 (see Fig. 10A) corresponding to classification A. As a result, in the

security information database 603, a record of "registration
No." = 3 (corresponding to security information 800) is added.
Further, the information management unit 1001 transfers the
security information 800 to the information disclosing unit
5 1003. As a result, the information disclosing unit 1003
registers the security information 800 in the disclosed
information database 1004.

At step SD7, the information management unit 1001
accesses the classification information database 606 by way
10 of the transfer unit 605, and retrieves the classification
information database 606 shown in Fig. 10C, using
classification A of the security information 800 as the key.
At step SD8, the information management unit 1001 judges
whether same classification as classification A of the
15 security information 800 is present or not in the
classification information database 606.

In this case, since the classification (A) of "the
developer" (developer 701A) in the classification
information database 606 coincides with the classification
20 A of the security information 800, the information management
unit 1001 judges Yes at step SD8. If judged No at step SD4,
the information management unit 1001 repeats the process after
step SD2.

At step SD9, the information management unit 1001
25 transfers the security information 800 addressed to the

developer client 700A to the transfer unit 605. As a result,
the transfer unit 605 transfers the security information 800
to the developer client 700A. In this case, the security
information 800 is not transferred to the developer client
5 700B. At step SD10, the information management unit 1001
judges if the reply information is received in the receiving
unit 607, and it is judged No in this case.

When the security information 800 is received by the
developer client 700A, the developers 701A judges if the
10 security information 800 is valid information or not. In
this case, suppose the developer 701A judges the security
information 800 to be valid. At the developer 701A, using
the developer client 700A, the reply information 801 (see
Fig. 9B), payment information 802 (see Fig. 9C), and patch
15 information 1100 (see Fig. 13C) are created, and they are
sent to the security information mediation apparatus 1000.
The reply information 801, payment information 802, and patch
information 1100 are received in the receiving unit 607 of
the security information mediation apparatus 1000 through
20 the network 702.

As a result, the information management unit 1001 judges
Yes at step SD10. At step SD11, the information management
unit 1001 judges if the patch information is received in the
receiving unit 607 or not, and it is judged Yes in this case.
25 At step SD17, the information management unit 1001 registers

the reply information 801 and patch information 1100 in the
reply information database 1002 (see Fig. 13A).

5 The information management unit 1001 transfers the
reply information 801 and patch information 1100 to the
information disclosing unit 1003. As a result, the
information disclosing unit 1003 registers the reply
information 801 and patch information 1100 in the disclosed
information database 1004 (see Fig. 13B). On the other hand,
if judged No at step SD11, the information management unit
10 1001 registers the reply information 801 in the replay
information database 1002 (see Fig. 13A).

At step SD13, the information management unit 1001
judges if the result of judgment of the reply information
801 shown in Fig. 9B is valid or not, and it is judged Yes
15 herein. At step SD14, the information management unit 1001
judges if the payment information 802 corresponding to the
reply information 801 is received in the receiving unit 607
or not, and it is judged Yes in this case. If judged No at
step SD14, the information management unit 1001 repeats the
20 same judgment.

At step SD15, the information management unit 1001
transfers the reply information 801 and payment information
802 to the transfer unit 608. As a result, the transfer unit
608 transfers the reply information 801 and payment
25 information 802 to the user client 501 through the network

information management unit 1001 has been received or not,
and if judged Yes, the disclosed information database 1004
is updated at step SE2.

If judged No at step SE1, on the other hand, going to
5 step SE3, the information disclosing unit 1003 judges if there
is an access request from the user client (in the diagram,
user client 901), and if judged No, the process after step
SE1 is repeated. If there is an access request from the user
client 901, the information disclosing unit 1003 judges Yes
10 at step SE3.

At step SE4, the information disclosing unit 1003, on
the basis of the disclosed information database 1004 (see
Fig. 13B), executes the process of displaying the information
disclosing screen 1200 shown in Fig. 14 in the display unit
15 (not shown) of the user client 901. This information
disclosing screen 1200 is a screen for disclosing the security
information ("reply information", "classification",
"content of security information", "replying person",
"correcting method") to the user 900.

20 At step SE5, the information disclosing unit 1003 judges
if desired security information is selected or not by the
user 900 from the information disclosing screen 1200, and
it is judged No in this case. At step SE8, the information
disclosing unit 1003 judges if the access is canceled or not,
25 specifically if an end button 1201 (see Fig. 14) is pressed

or not, and it is judged No in this case, and the process after step SE5 is repeated.

When the reply No. 3 shown in Fig. 14 is entered by the user 900, and the security information corresponding to reply No. 3 is selected, the information disclosing unit 1003 judges Yes at step SE5. At step SE6, the information disclosing unit 1003 retrieves the disclosed information database 1004 shown in Fig. 13, using reply No. 3 as the key, and security information pointer PS3 and patch information pointer PP3 are acquired.

Consequently, the information disclosing unit 1003, on the basis of the security information pointer PS3 and patch information pointer PP3, acquires the security information 800 and patch information 1100 from the disclosed information database 1004. At step SE7, the information disclosing unit 1003 transfers the security information 800 and patch information 1100 to the user client 901 through the network 502. Herein, when the end button 1201 is pressed by the user 900, the information disclosing unit 1003 judges Yes at step SE8, and the process after step SE1 is repeated.

When the security information 800 and patch information 1100 are received in the user client 901, the user 900 recognizes the content of the security information 800, and applies the patch program of the patch information 1100 to software X. As a result, software X is corrected.

000221" 5496260

In the fourth embodiment, by registering the classification information of the client information desired by the user 900 preliminarily in the information disclosing unit 1003, when the access is requested from the user client 5 901, the security information (patch information) corresponding to the classification information may be extracted from the disclosed information database 1004, and it may be disclosed to the user 900. Also in the fourth embodiment, in addition to the reply information 801 and 10 payment information 802, the patch information 1100 may be also transferred to the user client 501.

As described herein, according to the fourth embodiment, since the security information is disclosed by the information disclosing unit 1003, it may draw attention of a third party 15 (user 900) about presentation of security information, and presentation of multiple security information may be expected. Also according to the fourth embodiment, since the patch information 1100 is transferred to the user client 901 (user client 501), measures against security can be taken promptly.

20 The first to fourth embodiments of the invention have been described herein while referring to the accompanying drawings, but specific examples are not limited to the first to fourth embodiments alone, and design changes within the scope not departing from the true spirit of the invention 25 are also included in the invention.

For example, in the first to fourth embodiments, a security information mediation program for realizing the function of mediating security information may be recorded in a computer-readable recording medium 1400 shown in Fig. 17, and the security information mediation program recorded in this recording medium 1400 may be read in a computer 1300 shown in the same diagram, and executed to mediate the security information.

The computer 1300 shown in Fig. 17 comprises a CPU 1301 for executing the security information mediation program, an input device 1302 including keyboard and mouse, a ROM (read only memory) 1303 for storing various data, a RAM (random access memory) 1304 for storing operation parameters, a reading device 1305 for reading the security information mediation program from the recording medium 1400, an output device 1306 such as display and printer, and bus BU for connecting the devices and parts.

The CPU 1301 reads in the security information mediation program recorded in the recording medium 1400 through the reading device 1305, and executes the security information mediation program, and mediates the security information. The recording medium 1400 includes not only portable recording media such as optical disk, floppy disk, and hard disk, but also transfer medium for temporarily recording and holding the data such as the network.

As described herein, according to the invention, the security information from the information contributor is directly presented to the information recipient, and reward is paid to the contributor presenting useful security information, and therefore the environment is easy for the information contributor (user) to present security information, while the information recipient (for example, developer) can collect useful security information at low cost.

Furthermore, since only when the security information presented from the information contributor is new, such security information is transferred to the information recipient's terminal, it saves the wasteful time of transferring unnecessary security information to the information recipient's terminal, so that the security information may be collected efficiently.

Furthermore, by registering the classification information of the security information desired by the information contributor, and transferring the security information to the information recipient's terminal only when the classification information coincides with the classification result of the presented security information, it saves the wasteful time of transferring unnecessary security information, so that the security information may be collected more efficiently.

Furthermore, since the invalidity information showing
invalidity of the security information presented from the
information contributor is transferred to the information
contributor, it is effective to improve the service for the
5 user interested in the manner of use (valid or invalid) of
the presented security information.

Furthermore, since correction information as measure
for security information showing usefulness is transferred
to the information contributor, measures against security
10 information can be taken promptly.

Furthermore, since the security information is
disclosed, it may draw attention of a third party about
presentation of security information, and presentation of
multiple security information may be expected.

15 Furthermore, since the security information and
correction information are disclosed, it may draw attention
of a third party about presentation of security information,
and presentation of multiple security information may be
expected, and moreover measures against security information
20 can be taken promptly.

Although the invention has been described with respect
to a specific embodiment for a complete and clear disclosure,
the appended claims are not to be thus limited but are to
be construed as embodying all modifications and alternative
25 constructions that may occur to one skilled in the art which

	1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050	2051	2052	2053	2054	2055	2056	2057	2058	2059	2060	2061	2062	2063	2064	2065	2066	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	2077	2078	2079	2080	2081	2082	2083	2084	2085	2086	2087	2088	2089	2090	2091	2092	2093	2094	2095	2096	2097	2098	2099	2100	2101	2102	2103	2104	2105	2106	2107	2108	2109	2110	2111	2112	2113	2114	2115	2116	2117	2118	2119	2120	2121	2122	2123	2124	2125	2126	2127	2128	2129	2130	2131	2132	2133	2134	2135	2136	2137	2138	2139	2140	2141	2142	2143	2144	2145	2146	2147	2148	2149	2150	2151	2152	2153	2154	2155	2156	2157	2158	2159	2160	2161	2162	2163	2164	2165	2166	2167	2168	2169	2170	2171	2172	2173	2174	2175	2176	2177	2178	2179	2180	2181	2182	2183	2184	2185	2186	2187	2188	2189	2190	2191	2192	2193	2194	2195	2196	2197	2198	2199	2200	2201	2202	2203	2204	2205	2206	2207	2208	2209	2210	2211	2212	2213	2214	2215	2216	2217	2218	2219	2220	2221	2222	2223	2224	2225	2226	2227	2228	2229	2230	2231	2232	2233	2234	2235	2236	2237	2238	2239	2240	2241	2242	2243	2244	2245	2246	2247	2248	2249	2250	2251	2252	2253	2254	2255	2256	2257	2258	2259	2260	2261	2262	2263	2264	2265	2266	2267	2268	2269	2270	2271	2272	2273	2274	2275	2276	2277	2278	2279	2280	2281	2282	2283	2284	2285	2286	2287	2288	2289	2290	2291	2292	2293	2294	2295	2296	2297	2298	2299	2300	2301	2302	2303	2304	2305	2306	2307	2308	2309	2310	2311	2312	2313	2314	2315	2316	2317	2318	2319	2320	2321	2322	2323	2324	2325	2326	2327	2328	2329	2330	2331	2332	2333	2334	2335	2336	2337	2338	2339	2340	2341	2342	2343	2344	2345	2346	2347	2348	2349	2350	2351	2352	2353	2354	2355	2356	2357	2358	2359	2360	2361	2362	2363	2364	2365	2366	2367	2368	2369	2370	2371	2372	2373	2374	2375	2376	2377	2378	2379	2380	2381	2382	2383	2384	2385	2386	2387	2388	2389	2390	2391	2392	2393	2394	2395	2396	2397	2398	2399	2400	2401	2402	2403	2404	2405	2406	2407	2408	2409	2410	2411	2412	2413	2414	2415	2416	2417	2418	2419	2420	2421	2422	2423	2424	2425	2426	2427	2428	2429	2430	2431</
--	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	--------